Image of Client Logo

Penetration Testing Report

All Ports Tours Cruise Line (APT)

Prepared by: Our Company Name

September 17, 2025

CONFIDENTIAL

Table of Contents

1.0 Report Overview 4
1.1 Confidentiality 4
1.2 Legal Disclaimer 4
1.3 Contact Information 4
2.0 Executive Summary 5
2.1 Assessment Overview 5
2.1.1 Phases of Penetration Testing 5
2.2 Scoping and Time Limitations 6
2.3 Testing Summary 6
2.4 Tester Notes & Recommendations 6
3.0 Assessment Components 7
3.1 Open-Source Intelligence 7
3.2 External Penetration Test 7
3.3 Internal Penetration Test 7
4.0 Scope 8
4.1 Scope Exclusions 8
4.2 Client Allowances 8
4.3 Network Topology 8
5.0 Compliance Summary 9
5.1 Compliance1 9
5.2 Compliance2 9
6.0 Technical Finding Summary 10

7.0 Technical Findings . . . 11
7.1 Critical Risk Findings . . . 11
7.1.1 [Finding Name] . . . 11
7.2 High Risk Findings . . . 11
7.2.1 [Finding Name] . . . 11
7.3 Medium Risk Findings . . . 12
7.3.1 [Finding Name] . . . 12
7.4 Low Risk Findings . . . 13
7.4.1 [Finding Name] . . . 13
7.5 Informational Risk Findings . . . 14
7.5.1 [Finding Name] . . . 14
Example: Payment Card Industry Data Security Standard (PCI DSS) . . . 15
Appendix A: Social Engineering . . . 16
Methodology . . . 16
Results . . . 16
Appendix B: Methodologies . . . 17
Testing Frameworks . . . 17
Diagrams . . . 17
Appendix C: Attack Paths . . . 19
Visualizations . . . 19
Appendix D: Risk Assessment Metrics . . . 20
Appendix E: OSINT Assessment . . . 22
Findings . . . 22
Appendix F: Phishing Assessment . . . 23
Exercises . . . 23
Appendix G: Network Details . . . 24
Asset Inventory . . . 24

Appendix H: Tools Used **25**

Tool Table 25

1.0 Report Overview

Example: This report documents the results of a penetration test engagement for [Client Name]. It is intended for executive leadership, security teams, and technical staff. The test was conducted as a [black-box/gray-box/white-box] assessment to evaluate the security posture.

1.1 Confidentiality

Example: This document contains sensitive information related to the security of [Client Name]. It must not be distributed, copied, or disclosed without prior written permission. All findings remain the property of [Client Name].

1.2 Legal Disclaimer

Example: The penetration test was performed with full authorization from [Client Name]. While every effort was made to avoid disruption, unforeseen issues may occur. The testing team is not liable for damages resulting from remediation actions based on this report.

1.3 Contact Information

CLIENT ORGANIZATION	
Name	[Client Contact Name]
Role	[Client Role / Title]
Email	[Client Email]

TESTING TEAM	
Name	[Tester Name]
Role	[Senior Consultant]
Email	[Tester Email@cptc.team]

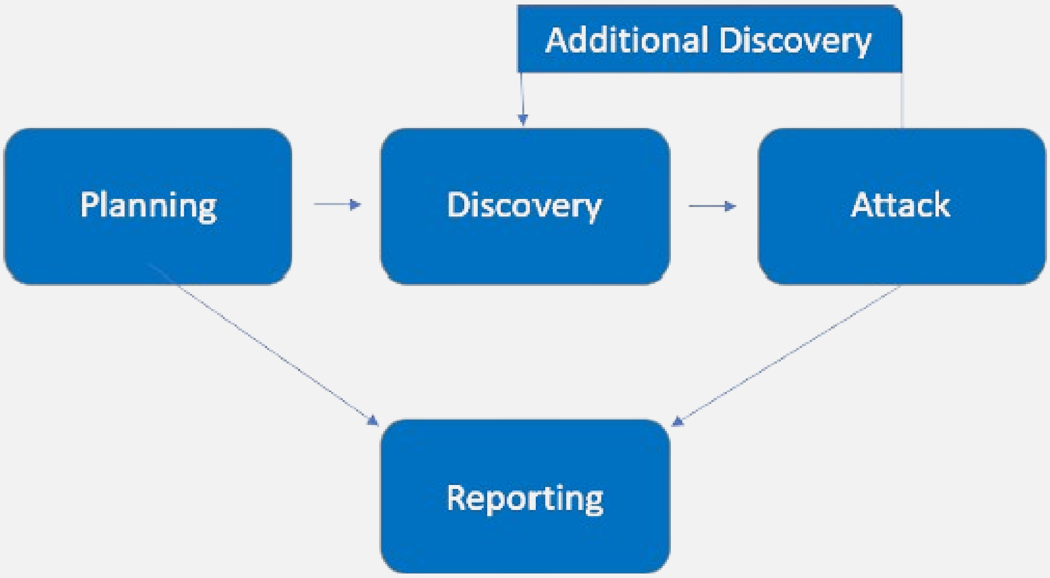
2.0 Executive Summary

2.1 Assessment Overview

Example: From February 22nd, 2021 to March 5th, 2021, Demo Corp engaged TCMS to evaluate the security posture of its infrastructure compared to current industry best practices that included an internal network penetration test. All testing performed is based on the NIST SP 800-115 Technical Guide, OWASP Testing Guide (v4), and customized frameworks.

2.1.1 Phases of Penetration Testing

- **Planning** – Customer goals and rules of engagement obtained.
- **Discovery** – Scanning and enumeration to identify vulnerabilities.
- **Attack** – Confirm vulnerabilities via exploitation.
- **Reporting** – Document findings, successes, and failures.



2.2 Scoping and Time Limitations

Briefly describe engagement scope, exclusions, and any time limitations.

2.3 Testing Summary

Example: The team conducted an internal network assessment of Demo Corp to evaluate its overall security posture. The assessment included vulnerability scanning of all provided IPs to determine patching health, common Active Directory attacks such as LLMNR poisoning, SMB relaying, IPv6 man-in-the-middle relaying, and Kerberoasting, as well as an evaluation of other risks including open file shares, default credentials, and sensitive information exposure. The team discovered that LLMNR was enabled, allowing the interception of user hashes, which were subsequently cracked via dictionary attacks, indicating a weak password policy. Using these credentials, the team accessed multiple machines, highlighting overly permissive user accounts. Older operating systems enabled WDigest attacks, exposing cleartext credentials, and reused local account hashes allowed additional machine access through pass-the-hash attacks. Lateral movement eventually led to the compromise of a Domain Administrator account. Additional critical risks included delegation attacks, SMB relay vulnerabilities, unrestricted IPv6 traffic, and unpatched devices with remote code execution vulnerabilities.

2.4 Tester Notes & Recommendations

Example: The findings suggest that Demo Corp is undergoing its first penetration test, with weak password policies and insufficient patch management being primary contributors to network compromise. The team recommends implementing stronger password policies, with a minimum of 15 characters for standard users and 30 for Domain Administrators, exploring password blacklisting, and considering a Privileged Access Management solution. Weak patching and outdated operating systems contributed to the compromise of multiple machines; therefore, Demo Corp should review patching recommendations, address vulnerabilities identified in the Technical Findings section, and improve patch management procedures. On a positive note, several attacks triggered alerts, indicating that the Security Operations team is actively monitoring the network. Overall, the network performed as expected for a first-time assessment, and the team recommends remediating all findings and conducting annual retesting to enhance the internal security posture.

3.0 Assessment Components

3.1 Open-Source Intelligence

Example tailor it more to the company though: OSINT emulates an attacker gathering publicly available information about the organization. Engineers collect data from websites, social media, and other sources to identify potential weaknesses and entry points.

3.2 External Penetration Test

Example tailor it more to the company though: An external penetration test emulates an attacker outside the organization's network. Engineers scan public assets to identify and exploit weaknesses.

3.3 Internal Penetration Test

Example tailor it more to the company though: An internal penetration test emulates an attacker from inside the network. Engineers scan internal hosts and perform internal network attacks.

4.0 Scope

The table below lists all workstations and hosts included in the scope of this assessment, along with their operating systems and IP addresses.

Workstation / Host Inventory	
OS	**IP Address**
Linux (Kali 2024.1)	10.10.10.11
Windows Server 2019	10.10.5.20
Windows 10	10.10.10.12

The table below summarizes the network subnets included in the scope, along with a brief description of each subnet's purpose.

Network Scope	
Subnet (CIDR)	**Description**
10.10.10.0/24	Tester workstations and pentest tools
10.10.5.0/24	Internal application servers (AD, DB, app servers)
203.0.113.0/28	Public-facing lab services (web, VPN)
10.10.1.0/24	Management network / admin workstations (out-of-scope)

4.1 Scope Exclusions

List systems excluded from testing.

4.2 Client Allowances

Describe client-provided access, credentials, or permissions.

4.3 Network Topology

Insert network diagrams for the engagement.

5.0 Compliance Summary

5.1 Compliance1

Compliance Info...

5.2 Compliance2

Compliance Info...

6.0 Technical Finding Summary

Unique ID	Finding	Severity	Impact / CVSS Score
VULN-001	Unpatched Web Server	High	7.6.
VULN-002	Weak Password Policy	Medium	5.4
VULN-003	Open SMB Share	High	7.3
VULN-004	Default Credentials on IoT Device	Medium	5.1
VULN-005	Example Vulnerability	High	7.9

7.0 Technical Findings

7.1 Critical Risk Findings

7.1.1 [Finding Name]

Do subsection for each critical finding

[Unique ID]: Service Account has weak password
Status: *Unremediated*
Findings Categorization: Critical
CVSS v4.0 Score: 9.3
CVSS Vector: `CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/V1:L/VA:H/SC:L/SI:L/SA:H/S:P`

Technical Description
Describe vulnerability in depth.

Business Impact Description
How this impacts the business and what effects this has.

Affected Systems
List systems.

Potential Compliance Violations
List compliance violations.

Remediation
Describe how to fix or patch vulnerability.

References
Provide links to websites, advisories, or CVEs.

Steps for Reproduction
Describe reproduction steps and reference relevant compliance frameworks.

7.2 High Risk Findings

7.2.1 [Finding Name]

Do subsection for each high finding

[Unique ID]: Service Account has weak password
Status: *Unremediated*
Findings Categorization: High
CVSS v4.0 Score: 7.2
CVSS Vector: `CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/V1:L/VA:H/SC:L/SI:L/SA:H/S:P`

Technical Description
Describe vulnerability in depth.

Business Impact Description
How this impacts the business and what effects this has.

Affected Systems
List systems.

Potential Compliance Violations
List compliance violations.

Remediation
Describe how to fix or patch vulnerability.

References
Provide links to websites, advisories, or CVEs.

Steps for Reproduction
Describe reproduction steps and reference relevant compliance frameworks.

7.3 Medium Risk Findings

7.3.1 [Finding Name]

Do subsection for each medium finding

[Unique ID]: Service Account has weak password
Status: *Unremediated*
Findings Categorization: Medium
CVSS v4.0 Score: 5.6
CVSS Vector: `CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/V1:L/VA:H/SC:L/SI:L/SA:H/S:P`

Technical Description
Describe vulnerability in depth.

Business Impact Description
How this impacts the business and what effects this has.

Affected Systems
List systems.

Potential Compliance Violations
List compliance violations.

Remediation
Describe how to fix or patch vulnerability.

References
Provide links to websites, advisories, or CVEs.

Steps for Reproduction
Describe reproduction steps and reference relevant compliance frameworks.

7.4 Low Risk Findings

7.4.1 [Finding Name]

Do subsection for each low finding

[Unique ID]: Service Account has weak password
Status: *Unremediated*
Findings Categorization: Low
CVSS v4.0 Score: 2.4
CVSS Vector: `CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/V1:L/VA:H/SC:L/SI:L/SA:H/S:P`

Technical Description
Describe vulnerability in depth.

Business Impact Description
How this impacts the business and what effects this has.

Affected Systems
List systems.

Potential Compliance Violations
List compliance violations.

Remediation
Describe how to fix or patch vulnerability.

References
Provide links to websites, advisories, or CVEs.

Steps for Reproduction
Describe reproduction steps and reference relevant compliance frameworks.

7.5 Informational Risk Findings

7.5.1 [Finding Name]

Do subsection for each informational finding

[Unique ID]: Service Account has weak password
Status: *Unremediated*
Findings Categorization: Informational
CVSS v4.0 Score: N/A
CVSS Vector: `N/A`

Technical Description

Describe vulnerability in depth.

Business Impact Description

How this impacts the business and what effects this has.

Affected Systems

List systems.

Potential Compliance Violations

List compliance violations.

Remediation

Describe how to fix or patch vulnerability.

References

Provide links to websites, advisories, or CVEs.

Steps for Reproduction

Describe reproduction steps and reference relevant compliance frameworks.

Appendix A: Non-Compliance Findings

Example: Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS Requirements	Related Findings
Protect Account Data	
Requirement 1: Password complexity not enforced for some user accounts	7.2.1
Requirement 2: Multi-factor authentication not enabled for administrative accounts	7.2.2
Data Encryption	
Requirement 3: Some sensitive files stored unencrypted on shared drives	7.1.2
Requirement 4: Backups of confidential data not encrypted at rest	
Vulnerability Management	
Requirement 5: Critical patches missing on Windows Server 2019	
Requirement 6: Web application subnet not scanned for vulnerabilities	

Appendix B: Social Engineering

Methodology

Include methodology, tests, and approach.

Results

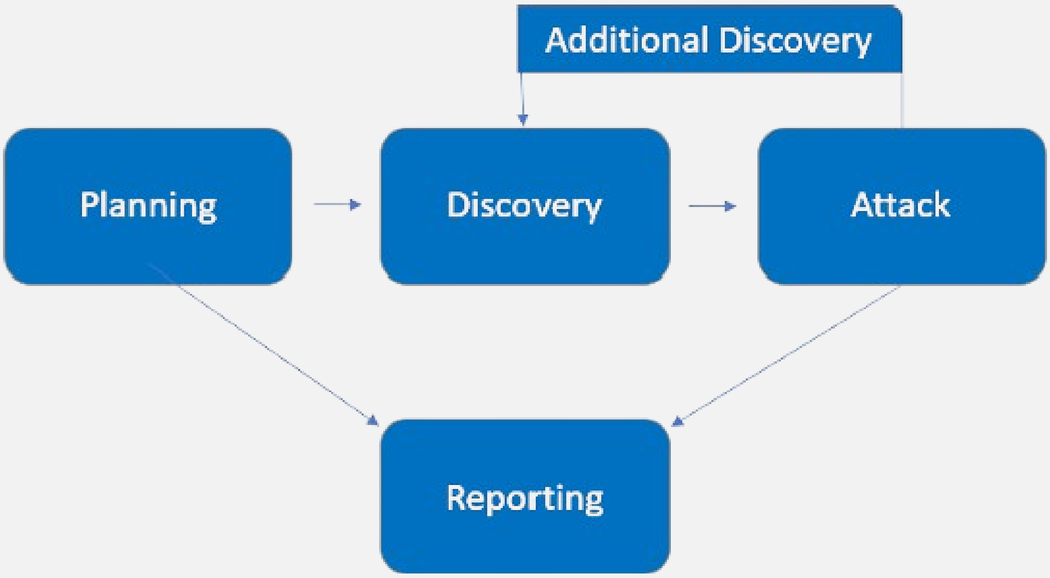
Include test outcomes, success rates, and notable findings.

Appendix C: Methodologies

Testing Frameworks

All testing performed is based on the NIST SP 800-115 Technical Guide, OWASP Testing Guide (v4), and customized frameworks.

Diagrams



Appendix D: Logical Systems

Logical Systems		
Logical System	**Abbreviation**	**Description**
Active Directory	AD	Centralized directory service for managing users, groups, and computers in a Windows environment.
Microsoft Exchange	EXCH	Email and calendaring server used for internal communications.
Kali Linux Pentest Workstation	KALI	Linux-based penetration testing workstation with security tools installed.
Windows Server 2019 Lab	WIN-SRV	Server used for lab applications, domain membership, and testing.
Web Application Lab	WEB	Simulated internal and public-facing web services for testing.
Database Lab	DB	Simulated database servers used for testing authentication, queries, and vulnerabilities.

Appendix E: Attack Paths

Visualizations

Illustrate attack chains and lateral movements.

Appendix F: Risk Assessment Metrics

CVSS 4.0 Severity Ratings

Score Range	Severity	Description
0.0	None	No impact, informational only.
0.1 – 3.9	Low	Minimal impact; exploitation unlikely to cause serious harm.
4.0 – 6.9	Medium	Moderate impact; may allow partial compromise or disruption.
7.0 – 8.9	High	Significant impact; exploitation could cause major disruption or breach.
9.0 – 10.0	Critical	Severe impact; straightforward exploitation with catastrophic consequences.

Impact Levels

Level	Name	Description
1	Insignificant	Minimal or no effect; cosmetic issues only.
2	Minor	Limited adverse effect; easily recoverable.
3	Moderate	Noticeable disruption; multi-hour outage or partial data exposure.
4	Major	Significant disruption, financial loss, or reputational impact.
5	Severe (Catastrophic)	Critical impact; long-term damage, legal penalties, or safety concerns.

Likelihood Levels

Level	Name	Description
1	Rare	Very unlikely; requires exceptional circumstances.
2	Unlikely	Possible but improbable; high exploitation complexity.
3	Possible	Could occur; known techniques or PoC exist.
4	Likely	Expected in many cases; active exploitation observed.
5	Almost Certain	Easy and widespread exploitation; automated tools.

Risk Matrix (Impact × Likelihood)

Likelihood ↓ / Impact →	1	2	3	4	5
1	Low	Low	Medium	Medium	High
2	Low	Medium	Medium	High	High
3	Low	Medium	High	High	Critical
4	Medium	High	High	Critical	Critical
5	Medium	High	Critical	Critical	Critical

Appendix G: OSINT Assessment

Findings

List name, description, business impact, source, mitigations, references, steps to reproduce.

Appendix H: Phishing Assessment

Exercises

Summarize phishing exercises and results.

Appendix I: Network Details

Asset Inventory

IP addresses, FQDNs, open ports, and other relevant information.

Appendix J: Tools Used

Tool Table

Include type (exploitation, post-exploitation, reconnaissance), description, and source.